



## DEPARTMENT OF DEFENSE

### Office of the Secretary

[Docket ID: DoD-2022-OS-0095]

### Privacy Act of 1974; System of Records

**AGENCY:** Department of Defense (DoD).

**ACTION:** Notice of a new system of records.

**SUMMARY:** In accordance with the Privacy Act of 1974, the Department of Defense (DoD) is establishing a new Department-wide system of records titled, “DoD Historical Records,” DoD-0014. This system of records covers DoD’s maintenance of records about individuals in the Department of Defense (DoD) historical system, the purpose of which is to collect, preserve, and present the history of the components within the DoD to support agency leadership and to inform the American public. Additionally, DoD is issuing a Direct Final Rule, which exempts this system of records from certain provisions of the Privacy Act, elsewhere in today’s issue of the *Federal Register*.

**DATES:** This system of records is effective upon publication; however, comments on the Routine Uses will be accepted on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. The Routine Uses are effective at the close of the comment period.

**ADDRESSES:** You may submit comments, identified by docket number and title, by any of the following methods:

\* Federal Rulemaking Portal: <https://www.regulations.gov>. Follow the instructions for submitting comments.

\* Mail: Department of Defense, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Regulatory Directorate, 4800 Mark Center Drive, Attn: Mailbox 24, Suite 08D09, Alexandria, VA 22350-1700.

*Instructions:* All submissions received must include the agency name and docket number for this *Federal Register* document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at <https://www.regulations.gov> as they are received without change, including any personal identifiers or contact information.

**FOR FURTHER INFORMATION CONTACT:** Ms. Rahwa Keleta, Defense Privacy and Civil Liberties Division, Directorate for Privacy, Civil Liberties and Freedom of Information, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Department of Defense, 4800 Mark Center Drive, Mailbox #24, Suite 08D09, Alexandria, VA 22350-1700; OSD.DPCLTD@mail.mil; (703) 571-0070.

**SUPPLEMENTARY INFORMATION:**

**I. Background**

DoD is establishing the “DoD Historical Records,” DoD-0014 as a DoD-wide Privacy Act system of records. A DoD-wide system of records notice (SORN) supports multiple DoD paper or electronic recordkeeping systems operated by more than one DoD component that maintain the same kind of information about individuals for the same purpose. Establishment of DoD-wide SORNs helps DoD standardize the rules governing the collection, maintenance, use, and sharing of personal information in key areas across the enterprise. DoD-wide SORNs also reduce duplicative and overlapping SORNs published by separate DoD components. The creation of DoD-wide SORNs is expected to make locating relevant SORNs easier for DoD personnel and the public, and create efficiencies in the operation of the DoD privacy program.

The mission of the DoD History Program is to collect, preserve, and present the history of the Department of Defense, in order to support Agency leadership and inform the American public. To further this mission, the Department is authorized to gather individuals’ information to prepare and publish historical reports, provide historically relevant information on advisory panels and commissions, organize historical presentations and prepare historical

studies. The DoD Historical Records SORN contains information on DoD civilian employees, uniformed service members, contractors, and other DoD-affiliated individuals. The system of records contains data derived from government records (Federal, state, and local), information collected directly from individuals, international government and non-government organizations, and publicly available information.

Additionally, DoD is issuing a Direct Final Rule to exempt this system of records from certain provisions of the Privacy Act elsewhere in today's issue of the *Federal Register*. DoD SORNs have been published in the *Federal Register* and are available from the address in **FOR FURTHER INFORMATION CONTACT** or at the Defense Privacy, Civil Liberties, and Freedom of Information Directorate website at <https://dpcl.d.defense.gov>.

## **II. Privacy Act**

Under the Privacy Act, a "system of records" is a group of records under the control of an agency from which information is retrieved by the name of an individual or by some identifying -number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined as a U.S. citizen or lawful permanent resident.

In accordance with 5 U.S.C. 552a(r) and Office of Management and Budget (OMB) Circular No. A-108, DoD has provided a report of this system of records to the OMB and to Congress.

Dated: August 29, 2022.

Aaron T. Siegel,  
Alternate OSD Federal Register  
Liaison Officer, Department of Defense.

**SYSTEM NAME AND NUMBER:** DoD Historical Records, DoD-0014.

**SECURITY CLASSIFICATION:** Classified and Unclassified.

**SYSTEM LOCATION:** Department of Defense (Department or DoD), located at 1000 Defense Pentagon, Washington, DC 20301-1000, and other Department installations, offices, or mission locations. Information may also be stored within a government-certified cloud, implemented, and overseen by the Department's Chief Information Officer (CIO), 6000 Defense Pentagon, Washington, DC 20301-6000.

**SYSTEM MANAGER(S):** The system managers are the Chief Historians assigned to components and commands throughout the Department. Their addresses will vary according to the location where the actions described in this notice are conducted. The Privacy Act responsibilities concerning access, amendment, and disclosure of the records within this system of records have been delegated to the DoD components. DoD components include the Military Departments of the Army, Air Force (including the U.S. Space Force), and Navy (including the U.S. Marine Corps), field operating agencies, major commands, field commands, installations, and activities. To contact the system manager at the DoD component with oversight of the records, go to [www.FOIA.gov](http://www.FOIA.gov) to locate the contact information for each component's Freedom of Information Act (FOIA) office.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:** 10 U.S.C. 113, Secretary of Defense; 44 U.S.C. § 2107 - Acceptance of Records for Historical Preservation; 44 U.S.C. 3101, Records Management by Federal Agencies; E.O. 12333, United States Intelligence Activities, as amended; and E.O. 12958, Classified National Security Information; and E.O. 9397, as amended.

**PURPOSE(S) OF THE SYSTEM:** The purpose of the DoD historical system is to collect, preserve, and present the history of the Agency and its components to inform the American public and archive historical information. DoD accomplishes this overall purpose by conducting the following activities:

A. Researching, writing, and publishing special historical studies, government reports, and book series.

B. Educating and training DoD personnel on historical information.

C. Accounting for and providing accurate information to inform DoD leaders and other government agency leaders and personnel on matters related to history.

D. Providing historical information to advisory panels and commissions.

E. Managing the DoD History Speaker Series in collaboration with Military Service and Joint Staff history programs.

F. Assisting in the production of public statements on behalf of DoD officials.

G. Supporting DoD libraries and museums with planning and/or undertaking historical, archival, curatorial, art, and archaeological programs and projects.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:** Individuals who participate in or are associated with historically relevant events. Individuals may include (but are not limited to) the following:

A. Current and former members of the uniformed services, including those in the National Guard or Reserve.

B. Current and former DoD civilian employees, contractors; or individuals (and their surviving beneficiaries) accorded benefits, rights, privileges, or immunities associated with DoD as provided by U.S. law.

C. Dependents and family members of uniformed services members.

D. Members of the public.

E. DoD “affiliated” individuals (e.g., non-appropriated fund employees working on DoD installations, Red Cross volunteers assisting at military hospitals, United Services Organization (USO) staff providing services on DoD installations, Congressional staff members visiting DoD installations, etc.).

**CATEGORIES OF RECORDS IN THE SYSTEM:**

A. Personal and biographical information including: name, date of birth; place of birth; immigration history, including date of naturalization; hometown; phone numbers, e-mail addresses, physical addresses; biographic information; information conveyed as physical images (photos/video), voice recordings (audio), and handwritten information.

B. Professional information, including: work history and professional experience (job titles, positions held, notable accomplishments); education; military experience, if applicable; civic duties; decorations; awards; employment identification, DoD ID Number, or badge number.

**RECORD SOURCE CATEGORIES:** Records and information stored in this system of records are obtained from:

A. Individuals.

B. Publicly available information including (but not limited to) newspapers, books, periodicals, magazines, television or movies, social media, industry or commercial databases, or other materials.

C. Government sources (Federal, state, local, tribal, foreign, and international).

D. Non-governmental organizations.

E. Classified or controlled unclassified sources including (but not limited to) intelligence products, law enforcement, security sources, and correspondence.

**ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING**

**CATEGORIES OF USERS AND PURPOSES OF SUCH USES:** In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, all or a portion of the records or information contained herein may specifically be disclosed outside the DoD as a Routine Use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government when necessary to accomplish an agency function related to this system of records.

B. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

C. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.

D. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

E. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

F. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

G. To appropriate agencies, entities, and persons when (1) the DoD suspects or confirms a breach of the system of records; (2) the DoD determines as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

H. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1)

responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

I. To another Federal, State or local agency for the purpose of comparing to the agency's system of records or to non-Federal records, in coordination with an Office of Inspector General in conducting an audit, investigation, inspection, evaluation, or other review as authorized by the Inspector General Act.

J. To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

**POLICIES AND PRACTICES FOR STORAGE OF RECORDS:** Records may be stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records may be stored locally on digital media; in agency-owned cloud environments; or in vendor Cloud Service Offerings certified under the Federal Risk and Authorization Management Program (FedRAMP).

**POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:** Records may be retrieved by name, DoD ID number, or other personal identifier.

**POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:** Records are to be retained by the Office of the Secretary of Defense, the Joint Staff, the Military Departments, the Defense Agencies, and the Defense Field Activities in accordance with their NARA-approved records retention schedules.

**ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:** DoD safeguards records in this system of records according to applicable rules, policies, and procedures, including all applicable DoD automated systems security and access policies. DoD policies require the use of controls to minimize the risk of compromise of personally identifiable information (PII) in paper and electronic form and to enforce access by those with a need to



know and with appropriate clearances. Additionally, DoD has established security audit and accountability policies and procedures which support the safeguarding of PII and detection of potential PII incidents. DoD routinely employs safeguards such as the following to information systems and paper recordkeeping systems: Multifactor log-in authentication including Common Access Card (CAC) authentication and password; physical token as required; physical and technological access controls governing access to data; network encryption to protect data transmitted over the network; disk encryption securing disks storing data; key management services to safeguard encryption keys; masking of sensitive data as practicable; mandatory information assurance and privacy training for individuals who will have access; identification, marking, and safeguarding of PII; physical access safeguards including multifactor identification physical access controls, detection and electronic alert systems for access to servers and other network infrastructure; and electronic intrusion detection systems in DoD facilities.

**RECORD ACCESS PROCEDURES:** Individuals seeking access to their records should follow the procedures in 32 CFR part 310. Individuals should address written inquiries to the DoD component with oversight of the records, as the component has Privacy Act responsibilities concerning access, amendment, and disclosure of the records within this system of records. The public may identify the contact information for the appropriate DoD office through the following website: [www.FOIA.gov](http://www.FOIA.gov). Signed written requests should contain the name and number of this system of records notice along with the full name, current address, and email address of the individual. In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the appropriate format:

If executed outside the United States: “I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature).”

If executed within the United States, its territories, possessions, or commonwealths:

“I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature).”

**CONTESTING RECORD PROCEDURES:** Individuals seeking to amend or correct the content of records about them should follow the procedures in 32 CFR part 310.

**NOTIFICATION PROCEDURES:** Individuals seeking to determine whether information about themselves is contained in this system of records should follow the instructions for Record Access Procedures above.

**EXEMPTIONS PROMULGATED FOR THE SYSTEM:** The DoD has exempted records maintained in this system from 5 U.S.C. 552a(c)(3); (d)(1)-(4); (e)(1), (e)(4)(G), (H), and (I); and (f) of the Privacy Act, pursuant to 5 U.S.C. 552a(k)(1). In addition, when exempt records received from other systems of records become part of this system, the DoD also claims the same exemptions for those records that are claimed for the system(s) of records from which they originated and claims any additional exemptions set forth here. An exemption rule for this system has been promulgated in accordance with the requirements of 5 U.S.C. 553(b)(1), (2), and (3), and (c), and published in 32 CFR part 310.

**HISTORY:** None.